Силабус курсу
ДОСЛІДЖЕННЯ І ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Ступінь вищої освіти – магістр
Рік навчання: 1
Семестр: 1
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Ігор Якименко
Контактна інформація	jiz@wunu.edu.ua

Опис дисципліни

Метою курсу Мета вивчення дисципліни "Дослідження і проектування систем захисту інформації" полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи та навчити їх застосуванню методів та засобів захисту інформації в умовах широкого використання сучасних інформаційних технологій.

Вивчення курсу "Дослідження і проектування систем захисту інформації» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Кібернетична безпека», «Криптографія», «Дискретна математика»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/1	Теоретичні засади дослідження та проектування систем захисту інформації	Принципи організації захисту інформації. Концепція національної безпеки України, концепція інформаційної безпеки України, доктрина інформаційної безпеки України. Основні поняття, терміни та визначення	Поточне опитування
2/1	Технічний захист інформації.	Технічний захист відомостей з обмеженим доступом. Технічна охорона об'єктів. Організація та контроль технічного захисту в Україні . Місце технічного захисту інформації у системі інформаційної безпеки. Сутність та завдання технічного захисту інформації.	Поточне опитування
2/1	Міжнародні стандарти у галузі інформаційної безпеки.	Стандарти і специфікації в галузі безпеки інформаційних систем. «Помаранчева книга» як оцінний стандарт. Класи безпеки інформаційних систем. Технічна специфікація X.800 Стандарт ISO/IEC 15408. Розвиток стандартів з управління ризиками. Стандарт ISO/IEC TR 13335	Поточне опитування

2/1	Теоретичні основи цілочисельної системи залишкових класів (СЗК)	Використовувати цілочисельну систему залишкових класів	Поточне опитування
2/1	Симетричний метод шифрування у СЗК та на основі Китайської теореми про залишки.	Застосовувати методи метод шифрування у СЗК	Поточне опитування
2/1	Асиметричний метод шифрування у СЗК.	Використовувати Асиметричний метод шифрування у СЗК	Поточне опитування
2/1	Нормалізована форма СЗК. Досконалі форми СЗК.	застосовувати методи	Поточне опитування
2/1	Міжбазисні перетворення на основі розмежованої СЗК	Застосовувати міжбазисні перетворення на основі розмежованої СЗК	Поточне опитування, тестування
2/1	Ступінчата СЗК. Метод шифрування у ступінчатій СЗК.	Застосовувати метод шифрування у ступінчатій СЗК	Поточне опитування
2/1	Дослідження стійкості симетричних алгоритмів шифрування у СЗК та на основі Китайської теореми про залишки.	Оцінювати стійкість симетричних алгоритмів шифрування у СЗК	Поточне опитування
2/1	Дослідження стійкості асиметричних методів шифрування у СЗК	Оцінювати стійкість асиметричних методів шифрування у СЗК	Поточне опитування
2/1	Метод пошуку оберненого поліному за модулем на основі методу невизначених коефіцієнтів	Використовувати метод пошуку оберненого поліному за модулем	Поточне опитування
2/1	Метод відновлення поліномів за його залишками	Використовувати метод відновлення поліномів за його залишками	Поточне опитування
2/1	Метод шифрування у поліноміальній системі залишкових класів	Застосовувати шифрування у поліноміальній системі залишкових класів	Поточне опитування
2/1	Дослідження стійкості методу шифрування у поліноміальній системі залишкових класів	Оцінювати стійкість методу шифрування у поліноміальній системі залишкових класів	Поточне опитування, тестування

Рекомендовані джерела інформації

1. Касянчук М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія) / М.Касянчук. – Тернопіль: ТНЕУ, 2019. – 224 с.

2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf, NIST Special Publication 800-12 Revision 1 An Introduction to Information Security Michael Nieles Kelley Dempsey Victoria Yan Pillitteri

3. Milov O., Kazakova N., Milczarski P., Korol O. Mechanisms of cyber security: the problem of conceptualization // Ukrainian Scientific Journal of Information Security, 2019, vol. 25, issue 2, pp. 110-116.

4. Information Security in an Organization Mohammed Mahfouz Alhassan, Alexander Adjei-Quaye International Journal of Computer (IJC) (2017) Volume 24, No 1, pp 100-116.

5. Спеціалізовані комп’ютерні технології в інформатиці. / під редакцією Николайчука Я.М.– Тернопіль: ТзОВ "Терно-граф".,2017 – С. 912.

6. Yakymenko I., Ivas'ev S., Kasianchuk M. High-Productivity Methods Of Finding Residues Multidigital Numbers By Modulo/ Колективна монографія/"Engineer of XXI Century" – the VI Inter University Conference of Students, PhD Students and Young Scientists, University of Bielsko-Biała (ATH) – Bielsko-Biała, Poland, 2016. – 922 p.

7. Etienne Lemaire. Pretty Modular Symmetric Encryption (PMSE), compact algorithm for "embedded cryptography" with quite low computational cost. 2019. ffhal-02131858

8. V. Migliore, M. M. Real, V. Lapotre, A. Tisserand, C. Fontaine and G. Gogniat, "Fast polynomial arithmetic for Somewhat Homomorphic Encryption operations in hardware with Karatsuba algorithm," *2016 International Conference on Field-Programmable Technology (FPT)*, Xi'an, China, 2016, pp. 209-212, doi: 10.1109/FPT.2016.7929535.

9. C. Jayet-Griffon, M. . -A. Cornelie, P. Maistri, P. Elbaz-Vincent and R. Leveugle, "Polynomial multipliers for fully homomorphic encryption on FPGA," *2015 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, Riviera Maya, Mexico, 2015, pp. 1-6, doi: 10.1109/ReConFig.2015.7393335.

10. Jianhua Wu, Hai Liu, Xishun Zhu Image encryption based on permutation polynomials over finite fields Optica Applicata, Vol. L, No. 3, 2020, pp. 357-376. DOI: 10.37190/oa200303

11. Alamsyah, A. Bejo, and T. B. Adji, "The replacement of irreducible polynomial and affine mapping for the construction of a strong S-box". *Nonlinear Dynamics*, vol. 93, no. 4, pp. 2105–2118, 2018.

12. Alamsyah, A. A Novel Construction of Perfect Strict Avalanche Criterion S-box using Simple Irreducible Polynomials May 2020 Scientific Journal of Informatics 7(1):10-22 DOI:10.15294/sji.v7i1.24006

13. P. Agarwal, A. Singh and A. Kilicman, "Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant", Advances in Mechanical Engineering, vol. 10, no. 7, pp. 1-18, 2018.

14. Kouther Fahad Alshammaria,* , Ayman Mostafaa , Shadi Nashwana Avalanche Analysis of Variant Polynomials for AES Turkish Journal of Computer and Mathematics Education Vol.12 No.14(2021), 2696- 2703

15. D. Schinianakis and T. Stouraitis, "Multifunction Residue Architectures for Cryptography," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 61, no. 4, pp. 1156-1169, April 2014, doi: 10.1109/TCSI.2013.2283674.

16. Tynymbayev, Sakhybay and Ibraimov, Margulan and Namazbayev, Timur and Gnatyuk, Sergiy, Development of Pipelined Polynomial Multiplier Modulo Irreducible Polynomials For Cryptosystems (February 25, 2022). Eastern-European Journal of Enterprise Technologies, 1 (4 (115)), 37–43, 2022, doi: https://doi.org/10.15587/1729-4061.2022.251913

17. Laurent-Stéphane Didier, Fangan-Yssouf Dosso, Nadia El Mrabet, Jérémy Marrez, Pascal Véron. Randomization of Arithmetic over Polynomial Modular Number System. 26th IEEE International Symposium on Computer Arithmetic, Jun 2019, Kyoto, Japan. pp.199-206, ff10.1109/ARITH.2019.00048ff. ffhal-02099713f

1. 18. Idris Abiodun Aremu, Kazeem Alagbe Gbolagade. Redundant Residue Number System Based Multiple Error Detection and Correction Using Chinese Remainder Theorem (CRT). Software Engineering. Vol. 5, No. 5, 2017, pp. 72-80. doi: 10.11648/j.se.20170505.12

Політика оцінювання

Політика щодо дедлайнів та перескладання: Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Використання друкованих і електронних джерел інформації під час контрольних заходів заборонено.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Оцінювання

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4
20%	20%	20%	40%
1. Усне опитування балів. 2. Письмова робота – max 50 балів. 3. Практичне завдання – max 30 балів	1. Усне опитування на заняттях – max 20 балів. 2. Письмова робота – max 50 балів. 3. Практичне завдання – max 30 балів	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Оцінка за тренінг – max 30 балів	1. Розв'язання 20 тестів по 3 бали = max 60 балів. 2. Практичне завдання = max 40 балів

Шкала оцінювання:

ECTS	**Бали**	**Зміст**
A	90–100	відмінно
B	85–89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом